

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-273936

(43)Date of publication of application : 26.09.2003

(51)Int.Cl.

H04L 12/66

G06F 13/00

(21)Application number : 2002-072754

(71)Applicant : FIRST TRUST:KK

(22)Date of filing : 15.03.2002

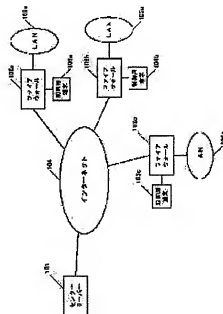
(72)Inventor : FUKUSHIRO SHIGEO
ARAKI MASAYUKI

(54) FIREWALL SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a packet filtering type firewall system which is easily operated.

SOLUTION: Each firewall device 102 performs packet filtering according to prescribed filtering rules, further monitors a packet which can be passed by the present filtering rules and, when the packet is judged to be refused, extracts a transmitting origin IP address from the header part of the packet and updates the filtering rules on the basis of extracted information. Furthermore, the transmitting origin IP address, etc., are recorded and periodically transmitted to a maintenance center server 101. The server 101 periodically processes the information transmitted from each device 102 statistically and transmits a refused IP address, etc., which is judged to be shared by a plurality of the devices 102 to each device 102. Each device 102 updates the filtering rules of itself, etc., on the basis of the information transmitted from the server 101.



[0002]

[Conventional Art] Conventionally, as a technology for
5 ensuring network security, a firewall has been known. The
firewall is placed between an external network such as
Internet and an internal network such as an in-enterprise
LAN and is a technique for blocking such as an intrusion
from the external network to the internal network by
10 controlling whether to permit communication for every data
based on a predefined standard.

[0003] Such a firewall has various systems, among which,
a packet filtering type firewall system is available. The
packet filtering type firewall system controls whether to
15 permit passing of every packet from an external network to
an internal network (or an internal network to an external
network). Such a control is performed in accordance with a
predetermined filtering rule.

[0004] Normally, under the filtering rule, a packet to
20 be a filtering target is identified by a transmission
source IP address, a destination IP address, a transmission
source port number, a destination port number, type of
protocol, and the like and an action (pass, rejection,
etc.) for the packet is designated.

(51) Int.Cl. ⁷	識別記号	F I	テマコード (参考)
H 0 4 L 12/66		H 0 4 L 12/66	B 5 B 0 8 9
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 Z 5 K 0 3 0

審査請求 未請求 請求項の数13 O L (全 14 頁)

(21) 出願番号 特願2002-72754(P2002-72754)

(22) 出願日 平成14年3月15日 (2002.3.15)

(71) 出願人 502094354

株式会社ファーストトラスト
広島県広島市安佐南区長東西五丁目2番13号

(72) 発明者 福城 茂生

広島県広島市安佐南区長東西五丁目2番13号
株式会社ファーストトラスト内

(72) 発明者 荒木 正之

広島県広島市安佐南区長東西五丁目2番13号
株式会社ファーストトラスト内

(74) 代理人 100111084

弁理士 藤野 義昭

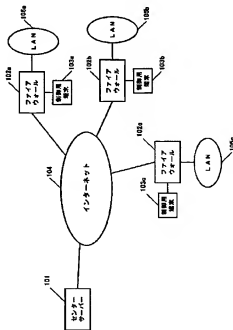
最終頁に続く

(54) 【発明の名称】 ファイアウォールシステム

(57) 【要約】

【課題】 運用するの容易なパケットフィルタリング型のファイアウォールシステムを提供する。

【解決手段】 各ファイアウォール装置102は、所定のフィルタリングルールに従ってパケットフィルタリングを行い、更に、現在のフィルタリングルールでは通過可能なパケットを監視し、当該パケットを拒否すべきと判定した場合は、当該パケットのヘッダ部から送信元IPアドレスを抽出し、抽出した情報に基づいてフィルタリングルールの更新を行う。更に、その送信元IPアドレス等を記録しておき、定期的に保守センターサーバー101に送信する。サーバー101は、各装置102から送られてくる情報を定期的に統計処理し、複数の装置102で共有すべきと判断される拒否IPアドレス等を、各装置102へ送信する。各装置102は、サーバー101から送られてきた情報に基づいて、自己のフィルタリングルール等を更新する。



【特許請求の範囲】

【請求項1】 保守センターサーバーと、複数のファイアウォール装置とが、ネットワークを介して接続されたファイアウォールシステムであって、

各ファイアウォール装置は、
自己が保持するフィルタリングルールに基づいて、パケットのフィルタリングを行うとともに、自己が受信したパケットに基づいて、当該パケットを拒否すべきか否かを判定し、拒否すべきと判定した場合は、当該パケットを拒否できるように、前記フィルタリングルールを更新し、

また、拒否すべきと判定したパケットに関する拒否パケット情報を保守センターサーバーへ送信し、

保守センターサーバーは、
各ファイアウォール装置から送られてくる拒否パケット情報を統計処理して、複数のファイアウォール装置で共有すべき拒否パケット識別情報を決定し、

複数のファイアウォール装置で共有すべき拒否パケット識別情報を、各ファイアウォール装置に送信し、
各ファイアウォール装置は、保守センターサーバーから送られてきた拒否パケット識別情報に基づいて、フィルタリングルールを更新することを特徴とするファイアウォールシステム。

【請求項2】 保守センターサーバーと、複数のファイアウォール装置とが、ネットワークを介して接続されたファイアウォールシステムであって、
各ファイアウォール装置は、自己の動作モード情報を保守センターサーバーへ送信し、

保守センターサーバーは、各ファイアウォール装置から送られてきた動作モード情報に合致する拒否パケット識別情報を、各ファイアウォール装置に送信し、
各ファイアウォール装置は、保守センターサーバーから送られてきた拒否パケット識別情報に基づいて、フィルタリングルールを生成し、当該フィルタリングルールに基づいて、パケットのフィルタリングを行うことを特徴とするファイアウォールシステム。

【請求項3】 フィルタリングルールに基づいて、パケットの通過を許可するか否かを制御するパケットフィルタリング部と、パケットを捕捉し、捕捉したパケットから必要な情報を抽出するパケット捕捉部と、
前記パケット捕捉部が抽出した情報に基づいて、捕捉したパケットが拒否すべきパケットであるか否かを判定し、拒否すべきパケットであると判定した場合、当該パケットから、フィルタリングルールを生成するのに必要な情報を抽出する判定部と、
当該判定部が抽出した情報に基づいて、前記フィルタリングルールを更新するルール更新部とを備えたことを特徴とするファイアウォール装置。

【請求項4】 前記判定部は、
パケットのデータに、予め決められた文字列が含まれて

いるか否かによって、拒否すべきパケットであるか否かを判定することを特徴とする請求項3に記載のファイアウォール装置。

【請求項5】 前記判定部は、
所定の時間内に、同一の送信元から所定数以上のメール・パケットを受信したか否か、及び、当該パケットが転送メールに関連するパケットであるか否かによって、拒否すべきパケットであるか否かを判定することを特徴とする請求項3に記載のファイアウォール装置。

【請求項6】 前記判定部は、
所定の時間内に、同一の送信元から所定の複数のポートに対するアクセスがあったか否かによって、拒否すべきパケットであるか否かを判定することを特徴とする請求項3に記載のファイアウォール装置。

【請求項7】 前記ルール更新部は、フィルタリングルールを更新した場合、当該フィルタリングルールを更新するのに必要な情報と、更新を行った原因と、更新を行った時刻を記録し、

当該記録を、外部ネットワークを介して、保守センターサーバーへ送信するデータ送信部を更に備えることを特徴とする請求項3～6のいずれか一項に記載のファイアウォール装置。

【請求項8】 前記ルール更新部は、フィルタリングルールを追加した場合、追加を行った時刻を記録しておき、その時刻から所定の時間が経過した後、追加したフィルタリングルールを削除することを特徴とする請求項3～6のいずれか一項に記載のファイアウォール装置。

【請求項9】 保守センターサーバーから送られてくる拒否パケット識別情報を受信するデータ受信部を更に備え、

前記ルール更新部は、前記拒否パケット識別情報に基づいて、前記フィルタリングルールを更新することを特徴とする請求項3～8のいずれか一項に記載のファイアウォール装置。

【請求項10】 保守センターサーバーから送られてくる拒否パケット識別情報を受信するデータ受信部を更に備え、

前記ルール更新部は、前記拒否パケット識別情報に基づいて、前記フィルタリングルールを更新し、

前記判定部は、前記拒否パケット識別情報に含まれる拒否文字列に基づいて、拒否すべきパケットであるか否かを判定することを特徴とする請求項4に記載のファイアウォール装置。

【請求項11】 パケットフィルタリングのためのフィルタリングルールを生成するプログラムであって、コンピュータをパケットを捕捉し、捕捉したパケットから必要な情報を抽出するパケット捕捉手段、

前記パケット捕捉手段が抽出した情報に基づいて、捕捉したパケットが拒否すべきパケットであるか否かを判定し、拒否すべきパケットであると判定した場合、当該パ

ケットからフィルタリングルールを生成するのに必要な情報を抽出する判定手段、及び当該判定手段が抽出した情報に基づいて、前記フィルタリングルールを生成するフィルタリングルール生成手段として機能させるためのプログラム。

【請求項12】 ファイアウォール装置から送られてくる拒否パケット情報を受信するデータ受信部と、受信した拒否パケット情報を記録する記録部と、記録された拒否パケット情報の統計処理を行う統計処理部と、

前記統計処理された情報から生成される拒否パケット識別情報を格納するデータベースと、前記データベースに格納された拒否パケット識別情報を、ファイアウォール装置に送信するデータ送信部とを備えたことを特徴とする保守センターサーバ。

【請求項13】 前記ファイアウォール装置から送られてくる情報には、当該ファイアウォール装置の動作モード情報が含まれ、

当該動作モード情報に基づいて、前記データベースに格納された拒否パケット識別情報を選択し、データ送信部に渡す選択部を更に備えることを特徴とする請求項12に記載の保守センターサーバ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、外部ネットワークと内部ネットワークの間で、パケットフィルタリングを行うファイアウォールシステムに関する。

【0002】

【従来の技術】 従来から、ネットワークセキュリティを確保するための技術として、ファイアウォールが知られている。ファイアウォールとは、インターネット等の外部ネットワークと、企業内LAN等の内部ネットワークとの間に置かれ、予め決められた基準に基づいて、各データについて通信を許可するか否かを制御することにより、外部ネットワークから内部ネットワークへの侵入等を阻止するための技術である。

【0003】 このようなファイアウォールには、様々な方式のものがあるが、そのうちの一つに、パケットフィルタリング型のファイアウォールがある。パケットフィルタリング型のファイアウォールは、パケット毎に、外部ネットワークから内部ネットワークへの（又は、内部ネットワークから外部ネットワークへの）通過を許可するか否かの制御を行うものであり、このような制御は、予め決められたフィルタリングルールに従って行われる。

【0004】 通常、フィルタリングルールでは、送信元IPアドレス、宛先IPアドレス、送信元ポート番号、宛先ポート番号、プロトコルの種類等によってフィルタリングの対象にするパケットが特定され、当該パケットに対する処置（通過、拒否等）が指定される。

【0005】

【発明が解決しようとする課題】 このようなフィルタリングルールは、管理者が予め設定する必要があるが、その設定作業には、ある程度のネットワーク等に関する知識が必要となり、一般ユーザには困難であった。また、そのような知識を有する者にとっても煩雑であった。

【0006】 本発明の目的は、運用するのが容易なパケットフィルタリング型のファイアウォールシステムを提供することにある。

【0007】

【課題を解決するための手段】 本発明に係るファイアウォールシステムは、保守センターサーバと、複数のファイアウォール装置とが、ネットワークを介して接続されたファイアウォールシステムである。

【0008】 そして、第一のファイアウォールシステムにおいては、各ファイアウォール装置は、自己が保持するフィルタリングルールに基づいて、パケットのフィルタリングを行うとともに、自己が受信したパケットに基づいて、当該パケットを拒否すべきか否かを判定し、拒否すべきと判定した場合は、当該パケットを拒否できるように、前記フィルタリングルールを更新し、また、拒否すべきと判定したパケットに関する拒否パケット情報を保守センターサーバへ送信する。保守センターサーバは、各ファイアウォール装置から送られてくる拒否パケット情報を統計処理して、複数のファイアウォール装置で共有すべき拒否パケット識別情報を決定し、複数のファイアウォール装置で共有すべき拒否パケット識別情報を、各ファイアウォール装置に送信する。そして、各ファイアウォール装置は、保守センターサーバから送られてきた拒否パケット識別情報に基づいて、フィルタリングルールを更新する。

【0009】 また、第二のファイアウォールシステムにおいては、各ファイアウォール装置は、自己の動作モード情報を保守センターサーバへ送信する。保守センターサーバは、各ファイアウォール装置から送られてきた動作モード情報に合致する拒否パケット識別情報を、各ファイアウォール装置に送信する。そして、各ファイアウォール装置は、保守センターサーバから送られてきた拒否パケット識別情報に基づいて、フィルタリングルールを生成し、当該フィルタリングルールに基づいて、パケットのフィルタリングを行う。

【0010】 本発明に係るファイアウォール装置は、フィルタリングルールに基づいて、パケットの通過を許可するか否かを制御するパケットフィルタリング部と、パケットを捕捉し、捕捉したパケットから必要な情報を抽出するパケット捕捉部と、前記パケット捕捉部が抽出した情報に基づいて、捕捉したパケットが拒否すべきパケットであるか否かを判定し、拒否すべきパケットであると判定した場合、当該パケットから、フィルタリングルールを生成するのに必要な情報を抽出する判定部と、当

該判定部が抽出した情報に基づいて、前記フィルタリングルールを更新するルール更新部とを備えたことを特徴とする。

【0011】この場合において、前記判定部は、パケットのデータに、予め決められた文字列が含まれているか否かによって、拒否すべきパケットであるか否かを判定するようにしてもよい。また、所定の時間内に、同一の送信元から所定数以上のメール・パケットを受信したか否か、及び、当該パケットが転送メールに関連するパケットであるか否かによって、拒否すべきパケットであるか否かを判定するようにしてもよい。また、所定の時間内に、同一の送信元から所定の複数のポートに対するアクセスがあったか否かによって、拒否すべきパケットであるか否かを判定するようにしてもよい。

【0012】また、前記ルール更新部は、フィルタリングルールを更新した場合、当該フィルタリングルールを更新するのに必要な情報と、更新を行った原因と、更新を行った時刻を記録するようにしてもよく、そして、前記ファイアウォール装置が、当該記録を、外部ネットワークを介して、保守センターサーバーへ送信するデータ送信部を更に備えるようにしてもよい。

【0013】また、前記ルール更新部は、フィルタリングルールを追加した場合、追加を行った時刻を記録しておき、その時刻から所定の時間が経過した後、追加したフィルタリングルールを削除するようにしてもよい。

【0014】また、前記ファイアウォール装置が、保守センターサーバーから送られてくる拒否パケット識別情報を受信するデータ受信部を更に備え、前記ルール更新部が、前記拒否パケット識別情報に基づいて、前記フィルタリングルールを更新するようにしてもよい。

【0015】また、前記判定部が、パケットのデータに、予め決められた文字列が含まれているか否かによって、拒否すべきパケットであるか否かを判定する場合は、ファイアウォール装置が、保守センターサーバーから送られてくる拒否パケット識別情報を受信するデータ受信部を更に備え、前記ルール更新部は、前記拒否パケット識別情報に基づいて、前記フィルタリングルールを更新し、前記判定部は、前記拒否パケット識別情報に含まれる拒否文字列に基づいて、拒否すべきパケットであるか否かを判定するようにしてもよい。

【0016】本発明に係るパケットフィルタリングのためのフィルタリングルールを生成するプログラムは、コンピュータを、パケットを捕捉し、捕捉したパケットから必要な情報を抽出するパケット捕捉手段、前記パケット捕捉手段が抽出した情報に基づいて、捕捉したパケットが拒否すべきパケットであるか否かを判定し、拒否すべきパケットであると判定した場合、当該パケットからフィルタリングルールを生成するのに必要な情報を抽出する判定手段、及び、当該判定手段が抽出した情報に基づいて、前記フィルタリングルールを生成するフィルタ

リングルール生成手段として機能させるためのプログラムである。

【0017】本発明に係る保守センターサーバーは、ファイアウォール装置から送られてくる拒否パケット情報を受信するデータ受信部と、受信した拒否パケット情報を記録する記録部と、記録された拒否パケット情報の統計処理を行う統計処理部と、前記統計処理された情報から生成される拒否パケット識別情報を格納するデータベースと、前記データベースに格納された拒否パケット識別情報を、ファイアウォール装置に送信するデータ送信部とを備えたことを特徴とする。

【0018】この場合において、前記ファイアウォール装置から送られてくる情報には、当該ファイアウォール装置の動作モード情報が含まれるようにしてもよく、そして、前記保守センターサーバーが、当該動作モード情報に基づいて、前記データベースに格納された拒否パケット識別情報を選択し、データ送信部に渡す選択部を更に備えるようにしてもよい。

【0019】

【発明の実施の形態】以下、本発明の実施の形態について、図面を参照しつつ詳細に説明する。

【0020】図1は、本発明によるファイアウォールシステムの全体構成を示す図である。

【0021】図1に示すように、本システムは、保守センターサーバー101と、複数のファイアウォール装置102（102a～102c）と、複数の制御用端末装置103（103a～103c）とを備える。

【0022】保守センターサーバー101及びファイアウォール装置102は、共に、インターネット104に接続されている。また、各ファイアウォール装置102は、それぞれ、内部ネットワーク105（105a～105c）に接続されている。

【0023】更に、各ファイアウォール装置102は、シリアルケーブルを介して、各制御用端末装置103と接続されている。制御用端末装置103は、ファイアウォール装置102の各種設定を行ったリ、ファイアウォール装置102の状態を確認したりするためのものである。

【0024】各ファイアウォール装置102は、外部ネットワークであるインターネット104と内部ネットワーク105との間で、パケットフィルタリングを行う。各ファイアウォール装置102は、予め決められたフィルタリングルールに従って、パケットフィルタリングを行うが、更に、現在のフィルタリングルールでは通過可能なパケットを監視し、当該パケットを通過させるのが望ましいか否かを判断する。そして、通過させるのが望ましくないとは判定した場合は、当該パケットから、フィルタリングルールを生成するのに必要な情報（例えば、送信元IPアドレス）を抽出し、抽出した情報に基づいて、当該パケットを拒否（遮断）できるようにフィルタ

リングルールの更新を行う。

【0025】フィルタリングルールを生成するのに必要な情報としては、送信元IPアドレス（又は、ドメイン名）、送信元ポート番号、宛先IPアドレス（又は、ドメイン名）、宛先ポート番号、プロトコル種類等があるが、以下では簡単のため、送信元IPアドレスで、フィルタリングルールを生成するのに必要な情報を代表させる。

【0026】本実施形態においては、各ファイアウォール装置102は、現在は通過可能なパケットに対して、3種類の判定を行う。

【0027】まず、第一に、各ファイアウォール装置102は、パケットのデータ（アプリケーション層のデータ）に、予め決められた文字列（拒否文字列）が含まれるか否かを判定する。そして、拒否文字列を含むパケットは、拒否すべきパケットであると判定する。

【0028】このような判定を行うことにより、例えば、教育機関のLAN環境において、児童の目に触れさせたくない文字列（悪質な言葉や差別用語等）を含むHTMLファイル等が児童が使う端末装置に表示されるのを防ぐことが可能になる。

【0029】第二に、各ファイアウォール装置102は、パケットが、スパムメールに関連するパケットであるか否かを判定する。スパムメールとは、不特定多数のユーザーに、一方的に送りつけられる宣伝メール等の電子メールのことをい、多くの場合、電子メールの不正中継が利用される。このようなスパムメールに関連するパケットについては、拒否することが望ましいので、各ファイアウォール装置102は、パケットが、スパムメールに関連するパケットであるか否かを判定する。スパムメールに関連するパケットであるか否かを判定する処理の詳細については後述する。

【0030】第三に、各ファイアウォール装置102は、パケットが、ポートスキャンに関連するパケットであるか否かを判定する。一般に、インターネットで利用される多くのサービスは、TCP又はUDPのサービスとして、サーバー上で稼働しており、TCPやUDPにはポート番号と呼ばれるサービス識別子が存在する。ポートスキャンとは、例えば、1番ポートから順番に接続を試みることで、スキャン対象のサーバーで稼働しているサービスが何なのかを調べるものである。このようなポートスキャンに関連するパケットについても、拒否することが望ましいので、各ファイアウォール装置102は、パケットが、ポートスキャンに関連するパケットであるか否かを判定する。ポートスキャンに関連するパケットであるか否かを判定する処理の詳細については後述する。

【0031】各ファイアウォール装置102は、以上のような判定の結果、拒否すべきパケットと判定した場合は、当該パケットの送信元IPアドレスを抽出して、抽

出した送信元IPアドレスに基づいて、当該送信元IPアドレスからのパケットを拒否できるようにフィルタリングルールを更新する。更に、その際、その送信元IPアドレス、更新原因（拒否文字列検出/スパムメール検出/ポートスキャン検出）、更新時刻等を記録しておく、当該記録（拒否パケット情報）を定期的に、保守センターサーバー101に送信する。

【0032】保守センターサーバー101は、各ファイアウォール装置102から送られてくる情報を記録し、記録した情報を定期的に統計処理する。そして、統計処理の結果、複数のファイアウォール装置102で共有すべきと判断される拒否パケット識別情報（例えば、拒否すべき送信元IPアドレス）を、各ファイアウォール装置102へ送信する。

【0033】各ファイアウォール装置102は、保守センターサーバー101から送られてくる拒否パケット識別情報を受け取ると、当該情報に基づいて、自己のフィルタリングルール等を更新する。

【0034】本ファイアウォールシステムでは、このような動作を行うので、各ファイアウォール装置102は、現在のフィルタリングルールでは対処できないパケットについても、ある程度、自律的に防御をすることが可能になる。また、あるファイアウォール装置102aにおいて、拒否すべきパケットの送信元と判定された送信元IPアドレスが、他のファイアウォール装置102b、102cでも共用されることとなり、他のファイアウォール装置102b、102cでは、自分で検出しなくても、望ましくないパケットを拒否するようにフィルタリングルールを更新することができ、望ましくないパケットの通過を未然に防ぐことが可能となる。

【0035】また、各ファイアウォール装置102は、自己の動作モード情報の一つとして、カテゴリと呼ばれる情報を有している。カテゴリは、制御用端末装置103を使って、管理者が設定（変更）することができる。

【0036】カテゴリは、例えば、ファイアウォール装置102が接続される内部ネットワーク105の種類（例えば、「教育機関」、「企業」、「個人」）や、セキュリティレベル（例えば、「高」、「中」、「低」）等に対応して予め定められる識別子（例えば、0000～9999のいずれか）である。

【0037】更に、各ファイアウォール装置102は、自己の動作モード情報として、「スパムメールをチェックするか」、「ポートスキャンをチェックするか」の情報を有しており、これらも、制御用端末装置103を使って、設定（変更）することができる。

【0038】各ファイアウォール装置102は、これらの動作モード情報を保守センターサーバー101へ送信する。なお、このとき、前述した拒否パケット情報等が存在すれば、これも同時に送信される。

【0039】保守センターサーバ101は、各ファイアウォール装置102から送られてくる動作モード情報を受け取ると、送られてきた動作モード情報に基づいて、当該動作モードに応じた拒否パケット識別情報（本実施形態においては、拒否文字列及び拒否送信元IPアドレス）を選択し、各ファイアウォール装置102に送り返す。

【0040】各ファイアウォール装置102は、保守センターサーバ101から送られてきた拒否パケット識別情報に基づいて、フィルタリングルールを生成し、また、拒否文字列の判定を行う。

【0041】本ファイアウォールシステムでは、このような動作を行うので、所望の動作モードを選択するだけで、自己のファイアウォール装置102に対して、適切なフィルタリングルール及び拒否文字列を自動的に設定することができ、各ファイアウォール装置102の管理者の負担が軽減される。

【0042】次に、以上のような動作を行う本ファイアウォールシステムを構成する各構成要素の詳細について説明する。

【0043】まず、ファイアウォール装置102の詳細について説明する。

【0044】図2は、ファイアウォール装置102のハードウェア構成例を示す図である。同図に示すように、ファイアウォール装置102は、CPU201と、メインメモリ202と、ROM203と、PCカードインタフェース部204と、シリアルインタフェース部205と、ネットワークインタフェース部206、207とを備える。

【0045】CPU201、メインメモリ202、ROM203、PCカードインタフェース部204、シリアルインタフェース部205、ネットワークインタフェース部206、207は、それぞれ、バス208に接続されている。また、PCカードインタフェース部204には、フラッシュATAカード209が接続される。シリアルインタフェース部205は、制御用端末装置103に接続され、ネットワークインタフェース部206は、外部ネットワーク（インターネット104）に接続され、ネットワークインタフェース部207は、内部ネットワーク105に接続される。

【0046】CPU201は、ファイアウォール装置102が行う各種処理を実行・制御する中央処理装置である。メインメモリ202は、CPU201が利用する各種プログラムやデータを格納する主記憶装置である。ROM203は、CPU201が利用するBIOS等を格納する記憶装置である。

【0047】PCカードインタフェース部204は、フラッシュATAカード209とバス208との間のデータのやり取りを制御するものである。シリアルインタフェース部205は、制御用端末装置103と、バス20

8と間のデータのやり取りを制御するものである。ネットワークインタフェース部206は、外部ネットワークとバス208との間のデータのやり取りを制御するものである。ネットワークインタフェース部207は、内部ネットワークとバス208との間のデータのやり取りを制御するものである。

【0048】フラッシュATAカード209は、CPU201が利用するオペレーティングシステム（OS）その他の各種プログラムやデータが記録された記録媒体である。なお、本実施形態においては、フラッシュATAカードの全記憶領域は、セクタ単位で暗号化が行われている。すなわち、ファイアウォール装置102のOS又はBIOSが、フラッシュATAカード209に対して、セクタ単位で読み書きを行う際、セクタデータに関して所定の復号/符号化を行う。このような処理を行うことにより、例えば、ファイアウォール装置102を、AT互換機等の一般的なパーソナルコンピュータ（PC）をベースに実現した場合であっても、フラッシュATAカード209に記録された情報が、他の同種のPC等で読み出されることを防止することが可能になる。

【0049】図3は、ファイアウォール装置102のソフトウェア構成例を示す図である。同図に示すように、ファイアウォール装置102は、パケットフィルタリング部301と、パケット捕捉部302と、判定部303～305と、フィルタリングルール制御部306と、データ送信部307と、データ受信部308とを備える。各部301～308は、基本的に、CPU201が、メインメモリ202にロードされたプログラムを実行することで実現される。

【0050】パケットフィルタリング部301は、TCP/IPプロトコルにおけるIPパケットを受け取り、パケットのヘッダの内容に応じて、受け取ったパケットを通過させるか否かの制御を行うものである。パケットフィルタリング部301は、フィルタリングルールを保持し、このフィルタリングルールに従って、受け取ったパケットを通過させるか否かを判断する。

【0051】フィルタリングルール制御部306は、パケットフィルタリング部301が保持するフィルタリングルールに新たなルールを追加したり、フィルタリングルールからあるルールを削除したりして、フィルタリングルールの制御を行う。

【0052】パケット捕捉部302は、パケットフィルタリング部301を通過したパケットを捕捉し、当該パケットの解析を行い、必要なデータを抽出して判定部303～305に渡す。パケット捕捉部302は、また、捕捉したパケットに関する記録を残すため、捕捉パケット記録テーブルを保持している。

【0053】図4は、捕捉パケット記録テーブルの構成例を示す図である。

【0054】同図に示すように、捕捉パケット記録テー

ブルは、「送信元」フィールド401と、「宛先」フィールド402と、「プロトコル」フィールド403と、「受信時刻」フィールド404とを備えている。

【0055】「送信元」フィールド401には、パケットの送信元のIPアドレス（及び、必要に応じてポート番号）が格納される。「宛先」フィールド402には、パケットの宛先のIPアドレス（及び、必要に応じてポート番号）が格納される。「プロトコル」フィールド403には、パケットのプロトコル種別を示す情報が格納される。「受信時刻」フィールド404には、パケットを受信した時刻が格納される。

【0056】パケット捕捉部302は、捕捉したパケットのヘッダ部を順次解析し、当該パケットがどのような種類のパケットかを判別する。そして、アプリケーション層のデータ（例えば、HTMLファイルの内容）を含むパケットについては、そのデータ部分を、TCP/IPヘッダと共に、判定部303に送る。また、電子メールに関連するパケットについては、そのメールヘッダを抽出し、TCP/IPヘッダと共に、判定部304に送る。また、ポートに対してアクセスを行うパケットについては、TCP/IPヘッダを判定部305に送る。各判定部303～305は、パケット捕捉部302から渡された情報に基づいて、捕捉したパケットが拒否すべきパケットであるかを判定する。

【0057】次に、捕捉したパケットが拒否すべきパケットであるかを判定する判定部303～305について説明する。本実施形態においては、3種類の判定部303～305が設けられている。

【0058】まず、判定部303について説明する。

【0059】判定部303は、パケットに含まれるアプリケーション層レベルのデータに、予め設定された文字列が含まれているか否かによって、当該パケットが拒否すべきパケットであるか否かを判定する。そのため、判定部303は、拒否すべき文字列のリスト（拒否文字列リスト）を保持している。

【0060】この拒否文字列リストは、ファイアウォール装置102の運用開始時に、管理者によって設定されたカテゴリに対応するものが、保守センターサーバー101からダウンロードされる。なお、運用開始時の拒否文字列リストについては、予めフラッシュATカード209に格納しておき、それを利用するようにしてもよい。

【0061】また、拒否文字列リストには、各ファイアウォール装置102を導入したサイト毎に、管理者が希望の文字列を追加等することもできる。そして、この拒否文字列リストは、定期的に（例えば、3日に一回）、他の情報と共に、保守センターサーバー101に送られる。更に、拒否文字列リストは、カテゴリ等、各ファイアウォール装置102の動作モード情報が変更された場合も、他の情報と共に、保守センターサーバー101に

送られる。

【0062】図5は、判定部303の判定処理の流れを示すフローチャートである。

【0063】図5に示すように、判定部303は、まず、パケット捕捉部302から渡されるTCP/IPパケットのデータに、拒否文字列リスト内の拒否文字列が存在するか否かを順次、判定する（S501）。

【0064】その結果、拒否文字列が含まれていなかった場合は（S501:NO）、そのまま処理を終了する。

【0065】一方、拒否文字列が含まれていた場合は（S501:YES）、当該パケットを拒否すべきパケットと判定し、当該パケットのヘッダ部から、送信元のIPアドレスを抽出する（S502）。そして、判定部303は、抽出した送信元IPアドレスと、当該パケットに含まれていた拒否文字列と、判定部303を表す識別子を、フィルタリングルール制御部306に渡して（S503）、処理を終了する。

【0066】以上のようにして、判定部303における判定処理が行われる。

【0067】次に、判定部304について説明する。

【0068】判定部304は、捕捉したパケットがスパムメールに関連するパケットであるか否かを判定する。具体的には、判定部304は、パケット捕捉部302から順次渡されるメールヘッダ及びTCP/IPヘッダを記録しておき、同一の送信元から、所定時間内に、所定数以上のメール・パケットを受信しているか否かであって、当該メールが転送メールである場合、当該メール・パケットがスパムメールに関連するパケットであると判定する。

【0069】図6は、判定部304の判定処理の流れを示すフローチャートである。

【0070】図6に示すように、判定部304は、まず、パケット捕捉部302から渡されるTCP/IPヘッダに基づいて、同一の送信元から、所定時間内に、所定数以上のメール・パケットを受信しているか否かを判定する（S601）。

【0071】その結果、同一の送信元から、所定時間内に、所定数以上のメール・パケットを受信していない場合は（S601:NO）、そのまま処理を終了する。

【0072】一方、同一の送信元から、所定時間内に、所定数以上のメール・パケットを受信していた場合は（S601:YES）、次に、メールヘッダに基づいて、当該メールが転送メールであるか否かを判定する（S602）。メールが転送メールであるか否かは、例えば、メールヘッダに「Received:」行が所定数以上含まれているか否かで判定する。

【0073】その結果、転送メールでなかった場合は（S602:NO）、そのまま処理を終了する。

【0074】一方、転送メールである場合は（S60

2: YES)、捕捉したパケットを拒否すべきパケットと判定し、当該パケットのヘッダ部から、送信元のIPアドレスを抽出する(S603)。そして、判定部304は、抽出した送信元IPアドレスと、判定部304を表す識別子を、フィルタリングルール制御部306に渡して(S604)、処理を終了する。

【0075】以上のようにして、判定部304における判定処理が行われる。

【0076】次に、判定部305について説明する。

【0077】判定部305は、捕捉したパケットがポートスキャンに関連するパケットであるかを判定する。具体的には、判定部305は、通常は使われることがないポート番号のリスト(拒否ポート番号リスト)を保持しており、更に、パケット捕捉部302から順次渡されるTCP/IPヘッダを記録しておき、同一の送信元から、拒否ポート番号リストに含まれる複数(所定数以上)のポートに対するアクセスが、所定の時間内にあった場合、ポートスキャンに関連するパケットであると判定する。

【0078】図7は、判定部305の判定処理の流れを示すフローチャートである。

【0079】図面に示すように、パケット捕捉部302からTCP/IPヘッダを受け取ると、判定部305は、まず、当該パケットが、ポートスキャンに関連するパケットであるかを判定する(S701)。

【0080】その結果、ポートスキャンに関連するパケットでないとは判定した場合は(S701:NO)、そのまま処理を終了する。

【0081】一方、ポートスキャンに関連するパケットであると判定した場合は(S701:YES)、当該パケットのヘッダ部から、送信元のIPアドレスを抽出する(S702)。そして、判定部305は、抽出した送信元IPアドレスと、判定部305を表す識別子をフィルタリングルール制御部306に渡して(S703)、処理を終了する。

【0082】以上のようにして、判定部305における判定処理が行われる。

【0083】各判定部303~305から拒否すべき送信元IPアドレス等が渡されると、フィルタリングルール制御部306は、当該送信元IPアドレスからのパケットを拒否できるように、パケットフィルタリング部301が保持するフィルタリングルールを更新する。

【0084】また、フィルタリングルール制御部306は、保守センターサーバー101へ送るため、各判定部303~305から渡される情報(拒否すべき送信元IPアドレス等)を順次記録しておく。

【0085】本実施形態においては、フィルタリングルール制御部306が追加するフィルタリングルールについて、一時的なものとするか、永久的なものとするか設定可能である。例えば、スパムメールやポートスキャン

ンについては、一時的に、その送信元からのパケットを拒否するだけで足りる場合があり、一度の不正アクセス等で、永久的に、その送信元からのパケットを拒否するようにすると、不都合な場合がある。

【0086】このような場合に対応できるようにするため、本実施形態では、各判定部303~305毎に、各判定部303~305が拒否すべきと判定した送信元IPアドレスからのパケットを、一時的に拒否するか、永久的に拒否するかを設定できる。そして、一時的拒否に設定された判定部から、拒否IPアドレス等が通知されると、当該拒否IPアドレスに基づいて、フィルタリングルールを追加した時刻を、当該拒否IPアドレスに対応させて記録しておき、追加後、予め決められた時間が経過したら、当該フィルタリングルールを削除する。このような構成とすることで、例えば、基本的には通信を確保したい送信元から、一時的にスパムメールやポートスキャン等があった場合に、当該送信元からのパケットを一時的に拒否して、必要な防御を達成しつつ、基本的には通信を確保したい送信元からのパケットを永久的に拒否する不都合を避けることが可能になる。

【0087】なお、フィルタリングルール制御部306は、フィルタリングルールを削除した時刻も、拒否IPアドレスに対応させて記録しておく。このようにフィルタリングルールを削除した時刻も記録しておくことにより、頻繁に追加・削除が繰り返される場合には、一時的な拒否とされていたものを、永久的な拒否に自動的に変更するように制御することも可能となる。

【0088】最後に、データ送信部307及びデータ受信部308について説明する。

【0089】データ送信部307は、必要な情報を保守センターサーバー101へ送信するためのものである。保守センターサーバー101へ送信される情報としては、フィルタリングルール制御部306に保持されている拒否IPアドレス、拒否文字列、フィルタリングルール追加時刻及びフィルタリングルール削除時刻等や、判定部303が保持する拒否文字列リストや、ファイアウォール装置102の動作モード情報等がある。

【0090】データ受信部308は、保守センターサーバー101から送信されてくる拒否パケット識別情報(拒否文字列及び拒否IPアドレス)を受信し、拒否文字列を判定部303に渡し、拒否IPアドレスをフィルタリングルール制御部306に渡す。

【0091】ファイアウォール装置102は、以上のような構成を有しているもので、望まないパケットを検出した場合に、自動的にフィルタリングルールを更新することが必要な防御を自律的に達成すること、及び、保守センターサーバー101との間で必要なデータのやり取りを行うこと等が可能となる。

【0092】次に、保守センターサーバー101の詳細について説明する。

【0093】図8は、保守センターサーバ101のハードウェア構成例を示す図である。同図に示すように、保守センターサーバ101は、CPU801と、メインメモリ802と、ハードディスクインタフェース部810と、ハードディスク装置811と、ネットワークインタフェース部806とを備える。

【0094】CPU801、メインメモリ802、ハードディスクインタフェース部810、ネットワークインタフェース部806は、それぞれ、バス808に接続されている。また、ハードディスクインタフェース部810には、ハードディスク装置811が接続されている。ネットワークインタフェース部806は、外部ネットワーク（インターネット104）に接続される。

【0095】CPU801は、保守センターサーバ101が行う各種処理を実行・制御する中央処理装置である。メインメモリ802は、CPU801が利用する各種プログラムやデータを格納する主記憶装置である。ハードディスク装置811は、CPU801が利用するOSその他の各種プログラムやデータを格納する補助記憶装置である。

【0096】ハードディスクインタフェース部810は、ハードディスク装置811とバス808との間のデータのやり取りを制御するものである。ネットワークインタフェース部806は、外部ネットワークとバス808との間のデータのやり取りを制御するものである。

【0097】図9は、保守センターサーバ101のソフトウェア構成例を示す図である。

【0098】同図に示すように、保守センターサーバ101は、データ受信部901と、記録部902と、統計処理部903と、拒否パケット識別情報データベース904と、送信データ選択部905と、データ送信部906とを備える。各部901～906は、基本的に、CPU801が、メインメモリ802にロードされたプログラムを実行することで実現される。

【0099】データ受信部901は、各ファイアウォール装置102から送られてくる情報を受信する。各ファイアウォール装置102から送られてくる情報には、各ファイアウォール装置102の現在の動作モード情報と、各ファイアウォール装置102で拒否すべきと判定したパケットに関する拒否パケット情報（フィルタリング制御部306が保持する情報）、各ファイアウォール装置102が現在使用している拒否文字列リスト（判定部303が保持）等が含まれる。

【0100】各ファイアウォール装置102から送られてきた拒否パケット情報は、記録部902に記録される。記録部902には、複数のファイアウォール装置102から送られてくる拒否パケット情報が順次記録される。統計処理部903は、記録部902に記録された拒否パケット情報を定期的に（例えば、一日一回）統計処理して、複数のファイアウォール装置102で共有すべ

き拒否パケット識別情報を決定し、拒否パケット識別情報データベース904に格納する。

【0101】図10は、拒否パケット識別情報データベース904の構成例を示す図である。

【0102】同図に示すように、本データベース904は、「カテゴリ」フィールド1001と、「データ種」フィールド1002と、「データ」フィールド1003と、「原因」フィールド1004とを備える。

【0103】「カテゴリ」フィールド1001には、カテゴリを識別する識別子（例えば、0000～9999のいずれか）が格納される。

【0104】「データ種」フィールド1002には、「データ」フィールド1003に格納されているデータの種類の示す情報が格納される。具体的には、「拒否文字列」であるか、「拒否IPアドレス」であるかを示す情報が格納される。

【0105】「データ」フィールド1003には、「データ種」フィールド1002に示されたデータの種類の対応して、拒否文字列又は拒否IPアドレスが格納される。

【0106】「原因」フィールド1004には、「データ」フィールドに格納されているIPアドレスが、いかなる原因で拒否すべきIPアドレスとされているのかわかる情報が格納される。具体的には、「スパムメール」に関連するものとして拒否すべきとされているのか、「ポートスキャン」に関連するものとして拒否すべきとされているのか等を示す情報が格納される。

【0107】送信データ選択部905は、「カテゴリ」フィールド1001と「原因」フィールド1004を使って、各ファイアウォール装置102から送られてきた動作モード情報に合致する拒否パケット識別情報を、拒否パケット識別情報データベース904から読み出す。そして、必要に応じて、読み出した拒否パケット識別情報と、各ファイアウォール装置102から送られてきた拒否パケット情報及び拒否文字列リストとを比較し、両者の差、すなわち、各ファイアウォール装置102が有していない拒否パケット識別情報を選択して、データ送信部906へ渡す。

【0108】データ送信部906は、送信データ選択部905から渡された拒否パケット識別情報を、データ受信部901から渡される送信元情報（送信元IPアドレス等）を使って、今回、拒否パケット情報等を送ってきたファイアウォール装置102へ返信する。

【0109】なお、保守センターサーバ101は、拒否パケット識別情報データベース904の「データ」フィールド1003に含まれているIPアドレスを有するホストが稼働（存在）しているか否かを、定期的に調べて、稼働（存在）していないと判断された場合は、拒否パケット識別情報データベース904から適宜削除する等、拒否パケット識別情報データベース904のメイン

テナンスも行う。

【0110】保守センターサーバー101は、以上のような構成を有しているため、各ファイアウォール装置102との間で必要なデータのやり取りを行うことが可能となる。

【0111】

【発明の効果】以上詳細に説明したように、本発明によれば、運用するのが容易なバケットフィルタリング型のファイアウォールシステムを提供することができる。

【図面の簡単な説明】

【図1】 本発明によるファイアウォールシステムの全体構成を示す図である。

【図2】 ファイアウォール装置102のハードウェア構成例を示す図である。

【図3】 ファイアウォール装置102のソフトウェア構成例を示す図である。

【図4】 捕捉バケット記録テーブルの構成例を示す図である。

【図5】 判定部303の判定処理の流れを示すフローチャートである。

【図6】 判定部304の判定処理の流れを示すフローチャートである。

【図7】 判定部305の判定処理の流れを示すフローチャートである。

【図8】 保守センターサーバー101のハードウェア構成例を示す図である。

【図9】 保守センターサーバー101のソフトウェア構成例を示す図である。

【図10】 拒否バケット識別情報データベース904の構成例を示す図である。

【符号の説明】

* 101 保守センターサーバー

102a~102c ファイアウォール装置

103a~103c 制御用端末装置

104 インターネット

105a~105c 内部ネットワーク

201 CPU

202 メインメモリ

203 ROM

204 PCカードインタフェース部

205 シリアルインタフェース部

206, 207 ネットワークインタフェース部

208 バス

209 フラッシュATAカード

301 バケットフィルタリング部

302 バケット捕捉部

303~305 判定部

306 フィルタリングルール制御部

307 データ送信部

308 データ受信部

20 CPU

802 メインメモリ

806 ネットワークインタフェース部

808 バス

810 ハードディスクインタフェース部

811 ハードディスク装置

901 データ受信部

902 記録部

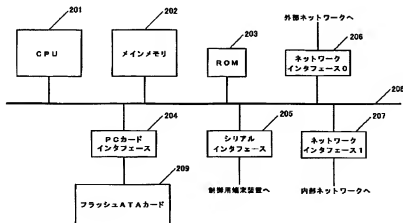
903 統計処理部

904 拒否バケット識別情報データベース

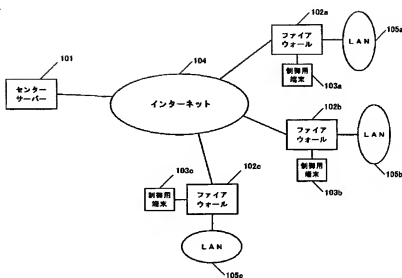
30 送信データ選択部

* 906 データ送信部

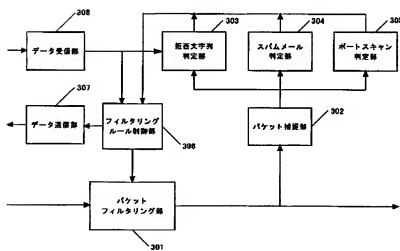
【図2】



【図1】



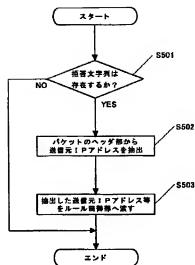
【図3】



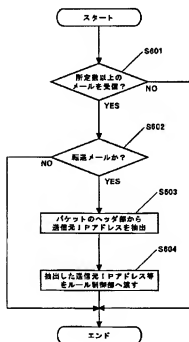
【図4】

401 送信元	402 宛先	403 プロトコル	404 受信時刻
AAA	BBB	UDP	XXX
CCC	DDD	TCP	YYY
EEE	FFF	TCP	ZZZ

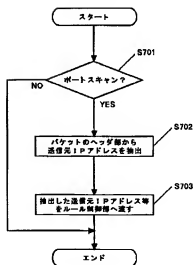
【図5】



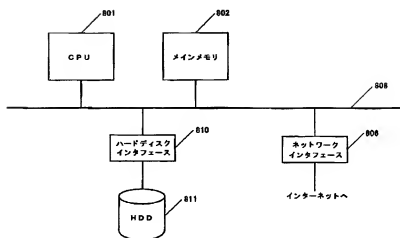
【図6】



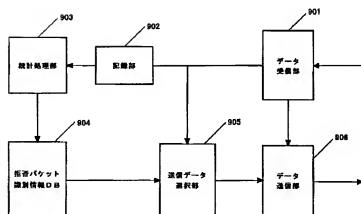
【図7】



【図8】



【図9】



【図10】

カテゴリ	データ型	データ	属性
0000	IP	AAAA	スパムメール
0000	IP	BBBB	ポートスキャン
0000	文字列	OOOO	—

フロントページの続き

Fターム(参考) 5B089 GA04 GA11 JB16 KA17 KB13
 MC08
 5K030 GA15 HA08 HD08 JA10 KX24
 LC14 LC15 MC07